Abstract

A method is proposed for protecting the central processing unit of a computer, in particular a smart card. Individual security-relevant registers are logically combined to form a check sum after the CPU has executed an instruction. Said check sum is stored and compared with an accordingly formed check sum before the onset of processing of the next instruction. If the compared check sums fail to match, this indicates manipulation of the register contents of the CPU in the time period between the execution of the two instructions. In such a case a corresponding error message is issued and the processor stopped or the card confiscated.